AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
INFORMATION ASSOCIATED WITH FACEBOOK ACCOUNT WWW.FACEBOOK.COM/LOUQUINCY.CARR.1 THAT IS STORED AT PREMISES CONTROLLED BY FACEBOOK, INC

Case No. 4:20 MJ 3258 NCC
SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of CALIFORNIA, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18:922(g); 924(c) & 1951	FELON IN POSSESSION OF A FIREARM; POSSESSION OF A FIREARM IN FURTHERANCE OF A CRIME OF VIOLENCE AND HOBBS ACT ROBBERY

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

B Freund 9/22/20

Bastian Freund, SA, FBI
Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: 09/22/2020

Judge's signature

City and state: St. Louis, MO

Honorable Magistrate Judge Noelle C. Collins
Printed name and title

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH FACEBOOK ACCOUNT WWW.FACEBOOK.COM/LOUQUINCY.CARR.1 THAT IS STORED AT PREMISES CONTROLLED BY FACEBOOK, INC.	)))))	No. 4:20 MJ 3258 NCC **FILED UNDER SEAL** SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Bastian Freund, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Criminal Procedure 41 for information associated with a certain Facebook user ID that is stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. The requested warrant would require Facebook to disclose to the United States records and other information in its possession, pertaining to the subscriber or customer associated with the user ID as further described in attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since 2003. I have been assigned to criminal investigations throughout my tenure as a Special Agent, predominantly working bank robberies, fugitives, carjackings, and Hobbs Act robberies. I am currently assigned to the St. Louis Division of the FBI's Violent Crime Task Force. During the course of my law enforcement experience, I have participated in numerous

investigations of violent crime. I am familiar with and have used normal methods of investigation, including, but not limited to, visual surveillance, questioning of witnesses, search and arrest warrants, informants, pen registers, precision location information, confidential sources and undercover agents, and court-authorized wire interceptions as well as GPS devices tracking in or on vehicles.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 922(g), 924(c), and 1951 have been committed by Louquincy **CARR**. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

LOCATION TO BE SEARCHED

6. The location to be searched is:

www.facebook.com/louquincy.carr.1 (hereinafter referred to as "Subject Account") located at 1601 Willow Road, Menlo Park, CA 94025, further described in Attachment A. The items to be reviewed and seized by the United States are described in Part II of Attachment B.

BACKGROUND RELATING TO FACEBOOK

7. The Internet is in part a computer communications network using interstate and foreign telephone and communication lines to transmit data streams, including data streams used to provide a means of communication from one computer to another and used to store, transfer and receive data and image files.

8. An "Internet Protocol" (IP) address is a unique series of numbers, separated by a period, that identifies each computer using, or connected to, the Internet over a network. An IP address permits a computer (or other digital device) to communicate with other devices via the Internet. The IP addresses aids in identifying the location of digital devices that are connected to the Internet so that they can be differentiated from other devices. As a mailing address allows a sender to mail a letter, a remote computer uses an IP address to communicate with other computers.

9. An "Internet Service Provider" (ISP) is an entity that provides access to the Internet to its subscribers.

10. The term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

11. Facebook is a business and company that operates as a remote computing service, a provider of electronic communications services through ISPs. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and

users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

12. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

13. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Membership in the group is monitored and regulated by the administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and creator of the group. Facebook uses the term "Group Contact Info" to describe the contact information for the group's creator and administrator, as well as the current status of the group profile page.

14. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

15. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook

users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Depending on the user's privacy settings, Facebook may also obtain and store the physical location of the user's device(s) as they interact with the Facebook service on those device(s). Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

16. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

17. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (*i.e.*, label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. Facebook allows users to edit or delete comments on their own profile pages, and users can adjust their profile settings to allow them to pre-approve comments on their own profile pages.

18. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

19. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

20. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

21. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

22. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

23. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

24. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

25. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

26. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. When a given Facebook account is deleted, Facebook retains certain information relating to that account for some period of time,

including user identity information, IP logs, and other data. Even if a given user deletes data, Facebook stores such data for extended periods of time on Facebook's servers.

27. Messages, photos, audio videos, and other records stored on Facebook server by a subscriber may not necessarily be located in the subscriber's home/work computer. The subscriber or user may store data on Facebook servers for which there is insufficient storage space in the subscriber's computer and/or which he/she does not wish to maintain in the computer at his/her residence or employment. A search of the files in the computer at the subscriber's residence or place of employment will not necessarily uncover the files that the subscriber has stored on the Facebook server. Therefore, the computers of Facebook are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and account application.

28. By their very nature, websites, social networking accounts, and internet-based applications described herein are kept and stored in computers and electronic-memory devices by the host companies, in addition to or in lieu of hard-copy versions of this data. Because such evidence is stored electronically, the data and evidence of the crimes described herein may be stored and be present for long periods of time.

29. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

30. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal

conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

PROBABLE CAUSE

31. On July 24, 2020, at approximately 5:30 P.M., a male Subject entered the T-Mobile store (a commercial establishment engaged in interstate or foreign commerce and in the business of buying and selling articles and commodities that have been previously transported in interstate or foreign commerce) located at 3630 South Grand Boulevard, St. Louis, Missouri, within the Eastern District of Missouri, and committed an armed robbery. The Subject was described by witnesses as a black male with a dark complexion, approximately 5'9" to 5'10", weighing approximately 230 to 240 pounds, having a goatee and tattoos on his arms. The Subject was wearing a white t-shirt, black sweatpants with a white stripe down the side, a dark blue "doo-rag" over his head, black tennis shoes, and a black fanny pack with a white logo draped across his shoulder. The Subject was also wearing a white surgical mask when he entered the store. The Subject looked at some display phones before approaching the counter. At the counter, the employee showed the Subject what appeared to be an iPhone in its box. The Subject pointed a silver semi-automatic handgun at the employee and demanded money from the register while also placing the boxed phone into his pants pocket. The employee complied and handed over United States Currency. After taking the money, the Subject picked up a bottle of hand sanitizer and poured it over the counter. The Subject then told the employee to take off the employee's shirt and wipe the counter of fingerprints. Thereafter, the Subject forced the employee into the back office at gunpoint. The Subject then fled the store on foot. Subsequent to the robbery, employees of the T-Mobile store conducted an audit and determined that the loss was approximately $1,200. Law enforcement received digital surveillance video documenting the robbery and processed the crime scene for forensic evidence.

32. On August 4, 2020, at approximately 1:15 P.M., a male Subject entered the same

T-Mobile store described above, located at 3630 South Grand Boulevard, St. Louis, Missouri, within the Eastern District of Missouri, and committed an armed robbery. The Subject was described by witnesses as a black male with a dark complexion, approximately 5'8" to 5'10", having a medium build. The Subject was wearing a black t-shirt, black baseball cap, grey shorts with a dark colored stripe down the side, and black shoes. Based on the video, it appeared the Subject had a white bag draped across over his chest. The Subject was wearing a light blue surgical mask when he entered the store. The Subject entered the store and looked around for a short time, appearing to be talking on a cellular phone. The Subject then approached an employee and produced a silver handgun, demanding the money from the register. The employee complied and removed the cash drawer from the register. While taking the United States currency from the register, the Subject also took a wallet, belonging to a customer that was laying on the counter. After taking the United States currency and the wallet, the Subject led two employees and two customers into a back room at gunpoint. The Subject then rummaged through some items in the office and placed an unknown item into his bag. The Subject then attempted to leave out a side door, but had difficulties in opening the door. One of the employees assisted the Subject in opening the door and the Subject ran through the parking lot and to the alley located to the east of the store. Subsequent to the robbery, employees of the T-Mobile store conducted an audit and determined that the loss was approximately $800. Law enforcement received digital surveillance video documenting the robbery and processed the crime scene for forensic evidence.

33. On August 14, 2020, at approximately 5:45 P.M., a male Subject entered a Boost Mobile store, located at 3706 South Grand Boulevard, St. Louis, Missouri, and committed an armed robbery. The Subject was described by witnesses as a black male with a dark complexion,

approximately 5'9", having a muscular build. The Subject was wearing a black baseball cap, black T-shirt, black track pants with a white stripe down the side, and black shoes. Based on the video, it appeared the Subject had a white bag draped across his chest and the Subject's baseball cap had a white color on the front. The Subject was wearing a blue surgical mask when he entered the store. The Subject entered the store and approached the employee at the register. After the employee and Subject had a conversation, the Subject produced a silver handgun and demanded money. The employee complied and removed United States currency from the register. After taking the United States currency from the first employee, the Subject turned to a second employee and demanded money from the second employee. The Subject then ordered the two employees to the rear of the store at gunpoint. Once in the back office, the Suspect asked where the bathroom was as well and if there was a rear exit. Thereafter, the Subject asked where the "good phones" were. The employees showed the Subject where new cell phones were located. One of the employees, at gunpoint, placed multiple phones into a bag the Subject had with him. After the bag was filled, the Subject ordered the two employees into the bathroom, then ran out the back door. Subsequent to the robbery, employees of the Boost Mobile store conducted an audit but a United States currency loss amount was not known. It was determined that the Subject took approximately fifteen iPhones. Law enforcement received digital surveillance video documenting the robbery and processed the crime scene for forensic evidence.

34. On August 25, 2020, at approximately 5:08 P.M., a male Subject entered a Wingstop Restaurant, located at 3626 South Grand Boulevard, Saint Louis, Missouri, and committed an armed robbery. Surveillance video showed the Subject was a black male, with a medium build, wearing black baseball cap with a white color on the front, what appeared to be a black t-shirt over a white t-shirt, and black track pants with a white stripe down the side. The

Subject was wearing a surgical mask when he entered the store. The Subject entered the restaurant while appearing to be talking on a cellular phone while walking around the restaurant, near the counter. The Subject waited for a short period of time, then walked behind the counter, removed a silver handgun from his pocket, and pointed it employees. The Subject ordered an employee to open the register and remove the money. The employee complied and handed the United States currency from the register to the Subject. The Subject then ordered an employee to open the safe. The employee complied and handed the Subject money from the safe. The Subject took the United States currency, then ordered all store employees into a back room of the restaurant. Once all employees were in the back room, the Subject ordered two employees to open the back door, at which time the Subject fled from the restaurant. An employee reported that $338.15 was taken from the register and $366 was taken from the safe. Law enforcement received digital surveillance video documenting the robbery and processed the crime scene for forensic evidence.

35. On August 13, 2020, the St. Louis Metropolitan Police Department Crime Laboratory advised that latent fingerprints recovered from the hand sanitizer bottle the Subject used in the July 24, 2020 robbery matched the right palm, index finger, and thumb of **CARR**.

36. Accordingly, on August 28, 2020, **CARR** was charged by complaint for committing the July 24, 2020, robbery described above. *See* United States v. Louquincy Carr, Case No. 4:20-MJ-6200 PAC. A federal arrest warrant was issued on that same date.

37. Law enforcement reviewed publicly accessible social media sites in order to try and identify a profile belonging to **CARR**. The **Subject Account** was located, having "vanity" name Louquincy Carr and, based on reviewing the profile photograph and other photographs and identifying information on the account page, it appeared to be **CARR's** Facebook page. A

review of the publicly viewable images and videos from the **Subject Account** showed **CARR** brandishing firearms and large sums of cash in several pictures. The **Subject Account** also contains several photographs of a female child that, based on **CARR's** posts, appeared to be his child. In two videos, both posted on August 20, 2020, **CARR** had a black fanny pack with a white logo draped over his shoulders, similar to the black fanny pack slung over the shoulder of the Subject in the charged robbery.

38. On September 8, 2020, the Hon. Nannette Baker issued search warrant for a residence located at 3433 Giles Avenue, Saint Louis, Missouri 63116. On September 10, 2020, law enforcement executed the search warrant and took **CARR** into custody. Also located at 3433 Giles Avenue were handguns, including what appears to be the silver handgun used in all four robberies.

39. On September 10, 2020, the Hon. Nannette Baker issued a search warrant for a residence located at 3729 Michigan Avenue, Saint Louis, Missouri. On September 10, 2020, law enforcement executed the search warrant and located clothing consistent with the clothing and bags CARR wore during the August 4, 2020 robbery and the bags CARR possessed during the July 24, August 4, and August 14, 2020 robberies.

40. During an interview with **CARR** on September 10, 2020, **CARR** identified the **Subject Account** as his Facebook account.

41. On September 17, 2020, a federal grand jury returned an indictment charging **CARR** with the four counts of armed robbery, in violation of Title 18, United States Code, Section 1951, four counts of brandishing a firearm in furtherance of a crime of violence, in violation of Title 18, United States Code, Section 924(c), and one count of felon in possession of

a firearm, in violation of Title 18, United States Code, Section 922(g). *See* United States v. Louquincy Carr, 4:20-CR-00550 AGF SPM.

42. A review of the publicly accessible information from the **Subject Account** reflects that the account is still active as of September 21, 2020. A preservation request for the Subject Account was sent to Facebook on August 19, 2020.

43. From my knowledge, training and experience, as well as discussions I have had with other agents and personnel familiar with computer-related investigations, I know that it is common for individuals engaged in the criminal activities described herein to use social networking sites such as Facebook to communicate with one another and facilitate their criminal activities. Such communications and the facilitation of criminal activities include the use of these applications and electronic and stored data that would identify and describe: (a) to communicate with associates before, during, and after their criminal activities, or to communicate with other non-involved third parties; (b) identify dates and locations where illegal activity has taken place or may take place in the future; (c) discussions concerning planning, operations, the transfer of information, concerning the illegal activities described herein as well as sharing photographs, videos, documents, and files; (d) financial transactions and monetary transfers used to facilitate and continue criminal activities as well as the existence and location of records, bank accounts, and businesses pertaining to those activities; (e) sales and purchases of equipment, materials, and goods related to the subject offenses as well as the location and use of assets accumulated; (f) travel, safe-houses, and locations where goods, materials and personnel stay or are kept; and (g) the existence of other communication facilities, including telephones, computers, e-mail and other electronic accounts used to by **CARR** or other associates to communicate.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

44. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the United States copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, United States-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

45. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on Facebook. Because the warrant will be served on Facebook, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

46. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

47. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution,

destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.

Respectfully submitted,

BASTIAN FREUND 9/22/20
Special Agent
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41, this 22nd day of September, 2020

The Honorable NOELLE C. COLLINS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Facebook account www.facebook.com/louquincy.carr.1 that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company located at 1601 Willow Road, Menlo Park, CA 94025.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f),

Facebook is required to disclose, from July 1, 2020 to September 21, 2020, the following information to the government for the account(s) and user ID(s) listed in Attachment A:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;

(b) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(c) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that account and user ID, including

the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

(d) All "check ins" and other location information;

(e) All IP logs, including all records of the IP addresses that logged into the account;

(f) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(g) All information about the Facebook pages that the account is or was a "fan" of;

(h) All past and present lists of friends created by the account;

(i) All information about the user's access and use of Facebook Marketplace;

(j) The types of service utilized by the user;

(k) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(l) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(m) All records pertaining to communications between Facebook and any person regarding the user or the account and user ID, including contacts with support services and records of actions taken.

(n) Any and all cookies associated with or used by any computer or web browser associated with the account, including the IP addresses, dates, and times associated with the recognition of any such cookie;

(o) All records of Facebook searches performed by the account;

(p) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(q) All photos and videos uploaded by that account and user ID and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

(r) All location data associated with the account created, uploaded, or shared by the account;

(s) All other records and contents of communications and messages made or received by the user, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests.

Facebook is hereby ordered to disclose the above information to the United States within 14 days of the date of this warrant.

II. Information to be seized by the United States

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 922(g), 924(c), and 1951 involving Louquincy **CARR** from July 1, 2020 to September 21, 2020, including, for each account or user ID identified on Attachment A, information pertaining to the following matters:

(a) The armed business robberies of T-Mobile located at 3630 South Grand Boulevard, St. Louis, Missouri, occurring on July 24, 2020 and August 4, 2020, Boost Mobile, located at 3706 South Grand Boulevard, St. Louis, Missouri on August 14, 2020, and Wingstop, located at 3626 South Grand Boulevard, Saint Louis, Missouri.

(b) The sale of any cellular devices between July 24, 2020 and September 21, 2020.

(c) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;

(d) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;

(e) The identity of the person(s) who created or used the account or user ID, including records that help reveal the whereabouts of such person(s).

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Facebook, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Facebook. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Facebook, and they were made by Facebook as a regular practice; and

b. such records were generated by Facebook's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Facebook in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Facebook, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date _____ Signature _____